REMARKS

The specification has been amended to correct a typographical error in paragraph [0126]. Independent claims 2 and 18 have been amended for clarification. No other claim has been amended, added or deleted, and no new matter has been added. Upon entry of the above amendments, claims 2-14 and 16-21 will remain in the application.

Claim Rejections – 35 U.S.C. §103(a)

Claims 2-14 and 16-21 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over Anderson et al. (US 2003/0002436) (hereinafter "Anderson") in view of Lin et al. (US 6,405,250) (hereinafter "Lin"). This rejection is traversed.

The claimed invention relates to a system and corresponding method for detecting the state of a computer network. As set forth in amended claim 2, the system includes:

> agents disposed in said computer network, each said agent comprising:
>
> data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network;
>
> means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said network in a normal state and activities of said network in an abnormal state; and
>
> means for comparing collected data to said activity models to determine whether said computer network is in said normal state or said abnormal state at different times and to dynamically update said activity models,
>
> wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network.

Claim 18 recites a corresponding method of detecting the state of a computer network. Such a system and method is not taught or suggested by Anderson and Lin taken separately or together.

In rejecting the claims over Anderson, the examiner alleged that Anderson discloses as system that detects the state of a computer network using agents identified as sensors 104 (see Figure 1). The examiner then alleged that each such agent (*i.e.*, sensor 104) includes the claimed "data collection means," "analyzing means," and "comparing means." Applicant submits that this is not the case and that the examiner has mischaracterized the teachings of Anderson.

Anderson teaches the use of sensors 104 to collect network traffic data. Some or all of the sensors 104 may be integrally disposed with routing devices 106. However, contrary to the examiner's allegations, the sensors 104 of Anderson do not perform the claimed analyzing and comparing functions. On the contrary, director 102 (Figure 3) includes the analyzer 304 and regulator 306. As described in paragraph [0045] of Anderson, analyzer 304 analyzes the network traffic data and alerts regulator 306 which determines where and what actions to be taken. As noted in paragraph [0022] of Anderson, each director 102 is assigned responsibility for a subset of sensors 104 and selectively activates/deactivates the sensors 104 in addition to determining whether the network link of interest is suspicious of being abused or misused (for example, the source addresses of the network traffic routed over the network link of interest are even layered on top of the normal traffic pattern; see paragraph [0034]). In any case, the disclosure of Anderson is quite clear that sensors 104 are not performing any analyzing and comparing functions as the examiner alleges. Rather, the processing functions of Anderson are performed by the director 102. As such, Anderson does not teach the claimed agents.

Since the processing is performed by director 102 for data received from a plurality of sensors 104, it is clear that Anderson does not teach comparing the results of the pattern analysis of data collected by one agent (sensor 104) to the results of pattern analysis of data collected by analyzing means of other agents to "identify similar patterns of suspicious activity in different portions of the computer network" as claimed. For starters, sensors 104 do not perform any pattern analysis; therefore, sensors 104 could not perform any comparisons of the results of such pattern analyses. Anderson also does not teach that director 102 compares the results of pattern analysis of data from one agent with the results of pattern analysis from another agent to "identify similar patterns of suspicious activity in different portions of the computer network" as claimed. On the contrary, any "analysis" performed by the director 102 is for determining whether a network link of interest is "suspicious of being abused or misused." Anderson provides no way to extrapolate this finding to determine the status of the entire computer network as claimed.

Moreover, as acknowledged by the examiner at page 4 of the Official Action, Anderson "lacks or does not expressly disclose developing activity models representative of activities of said network." For such teachings, the examiner refers to the general teachings of Lin of utilizing "behavior transition models" relating to network-wide behaviors leading to state transitions. Applicant submits that such models do not represent activities of the network in a "normal state" and activities of the network in an "abnormal state" for a determination by a comparing means as to whether the network is in a "normal state" or an "abnormal state" as claimed. The teachings of Anderson are no help either, for Anderson teaches determining whether a traffic pattern is consistent with an expected pattern, not a determination of whether a computer network is in a "normal state" or an "abnormal state" as claimed.

Accordingly, neither Anderson nor Lin teaches a system that detects the state of a computer network, where the system comprises not one, but plural "***agents***" disposed in a computer network, where "***each said agent"*** includes "comparing means [that] compares the results of the pattern analysis of data collected by ***an agent*** to the results of pattern analysis of data collected by analyzing means of ***other agents*** to identify similar patterns of suspicious activity in ***different portions of the computer network***" as claimed in independent claims 1 and 18. No such plural agents with such features are taught by Anderson and/or Lin. The examiner's conclusions to the contrary are not supported by the teachings of Anderson and Lin.

For at least these reasons, even if the teachings of Anderson and Lin could have been combined by one skilled in the art as the examiner alleged, the claimed system and method would not have resulted. The rejection of claims 2-14 and 16-21 as being unpatentable as obvious over Anderson in view of Lin is believed to be improper and withdrawal of this rejection is respectfully solicited.

Conclusion

For the reasons set forth herein, claims 2-14 and 16-21 are believed to be in condition for allowance. A Notice of Allowability is solicited.

Date: Monday, October 26, 2009

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439